NURX.

548 Market Street, Suite #94061
San Francisco, California 94104-5401
privacy@nurx.co

April 20, 2023

[redacted]

Dear [redacted]

At Propel Network, LLC d/b/a Nurx ("Nurx"), we value and respect the privacy of your information, which is why we are writing to inform you of a recent incident that may have involved your information. Nurx partners with CVS Specialty, Inc. ("CVS") to provide certain services and medication to eligible CVS members (the "members"). The Nurx website uses "pixels" and similar common technologies ("Tracking Technologies"), such as those made available by Google, Meta (Facebook), and TikTok (the "Third Parties"). Nurx recently became aware that its use of Tracking Technologies and data sharing practices may have allowed more member information to be disclosed to the Third Parties than permitted by Nurx's agreement with CVS. In some cases, this disclosure may have permitted the Third Parties to identify members without authorization.

As soon as we learned of this, we launched an internal review to evaluate Nurx's use and disclosure of member information collected by our website and to determine what information may have been impermissibly disclosed to the Third Parties as a result. Nurx's investigation determined that certain member information that may be regulated as protected health information ("PHI") under HIPAA may have been disclosed to the Third Parties without having obtained the appropriate authorization or consent under HIPAA. Nurx has since updated the CVS member-specific website flow (the "Workflow") and can confirm that member data in the Workflow is no longer shared with any Third Parties, unless permitted under applicable law or with your permission.

Although we have no evidence to suggest that any information has or will be misused by any Third Party, and not all members' data was disclosed, we are notifying you out of an abundance of caution because this incident, by its nature, could have allowed the Third Parties to impermissibly access, use, and/or disclose your information.

WHAT INFORMATION WAS INVOLVED?

Based on our investigation, between November 1, 2021 and December 22, 2022, the following type of information may have been shared with Third Parties: your hashed full name, hashed phone number, hashed email address, hashed unique identification number, page views (including, in some instances, the website URL), IP address, and information that could relate to your medical condition.

WHAT WE ARE DOING

As noted above, Nurx immediately launched a comprehensive review to evaluate and resolve any impermissible disclosures. We can confirm that as of December 22, 2022, all sharing of CVS member information with the Third Parties in the Workflow has ceased. Nurx is also working with Third Parties to ensure that proper contractual obligations are in place where applicable to protect patient information and is committed to only sharing members' information with Third Parties in a manner that complies with Nurx's agreement with CVS and applicable laws. Additionally, our comprehensive analysis of our website and information disclosure practices continue and we are committed to making changes that further protect member information.

WHAT YOU CAN DO

Again, we have no evidence to suggest that any information has or will be misused by any Third Party but are notifying you out of an abundance of caution. While you are not required to take any action, as a general matter, the following practices can help to protect your medical information.

- Review your Explanation of Benefits (EOB) statement, which you can receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the EOB statement and ask for copies of medical records from November 3, 2021 and December 22, 2022.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

Even though the information involved in this incident does not affect your credit and we have no evidence to suggest that your information has been or will be misused, we are required by law to provide you with certain information about identity theft. Please review the enclosed "Additional Resources" document included with this letter for further steps you can take to protect your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. It is also recommended that you remain vigilant for potential incidents of fraud and identity theft by reviewing your account statements and monitoring your credit reports for unauthorized activity.

FOR MORE INFORMATION

For further information and assistance, please contact our dedicated incident response line at (800) 321-NURX and select option 3 between 9 a.m. – 9 p.m. Eastern Time, Monday through Friday, or email us at privacy@nurx.co.

Very Respectfully,

Channin Gladden
Sr Manager, Governance, Risk, and Compliance
Propel Network, LLC d/b/a Nurx

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's (FTC) website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alert. You have the right to place an initial or extended "fraud alert" on your file at no cost by contacting any of the three nationwide credit reporting agencies identified above. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert displayed on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. If you are a victim of identity theft and have filed an identity theft report with law enforcement, you may want to consider placing an extended fraud alert, which lasts for 7 years, on your credit file.

Security Freeze. You have the right to place, lift, or remove a "security freeze" on your credit report, free of charge. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or up to 3 business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within 5 business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through

a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the 3 credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to remove the security freeze.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC, proper law enforcement authorities and/or your state attorney general. You may also contact these agencies for information on how to prevent or avoid identity theft and to obtain additional information about fraud alerts and security freezes. You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (438-4338).

- **For California Residents**: You may also wish to review the information provided by the California Attorney General at https://oag.ca.gov/idtheft.
- **For Maryland Residents**: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, Telephone: 1- 410-576-6491 or 1-888-743-0023.
- **For New Mexico Residents**: You have rights pursuant to the Fair Credit Reporting Act ("FCRA"), such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the FCRA not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-_fcra.pdf, or by

writing Consumer Response 30-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

- **For New York Residents**: You may obtain additional information about security breach response and identity theft prevention and protection from the New York State Office of the Attorney General at https://ag.ny.gov/ or by calling 1-800-771-7755; the New York State Police at http://troopers.ny.gov/ or by calling 1-518-457-6721; and/or the New York Department of State at https://www.dos.ny.gov or by calling 1-800-697-1220.
- **For North Carolina Residents**: You may obtain additional information about preventing identity theft provided by the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/identity-theft/, by calling 1-877- 566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.
- **For Oregon Residents**: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at https://doj.state.or.us, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.
- **For Rhode Island Residents**: You have the right to file and obtain a copy of any police report. You also have the right to request a security freeze as described above. You may contact the Rhode Island Attorney General at http://www.riag.ri.gov, by calling 401-274-4400, or by writing to 150 South Main Street, Providence RI 02903. There are nine (9) Rhode Island residents potentially impacted by this incident.
- **For District of Columbia Residents**: You may obtain information about avoiding identity theft from the Office of the Attorney General for the District of Columbia by visiting https://oag.dc.gov/consumer-protection, emailing consumer.protection@dc.gov, calling (202) 442-9828, or mailing Office of the Attorney General, Office of Consumer Protection 400 6th Street, NW Washington, DC 20001.